

IP-Granite

Layer-3 Virtual Private network

INTRODUCTION

IP-Granite is a Secured Virtual Private Network (S-VPN) solution that secures IP-based network traffic over a public network. IKEv2/IPsec is the underlying technology that provides the confidentiality and authenticity for the Site-to-Site solution. The Road Warrior solution uses Transport Layer Protocol (TLS).

IP-Granite is a fully in-house developed product from **ECNanoteq**. It leverages on the security and technical expertise built over more than 30 years. **IP-Granite** provides organisations the possibility to customise cryptographic algorithms. The product can be supplemented with a QCM-G, **ECNanoteq**'s high-speed hardware cryptographic module. This module is part of a family of hardware cryptographic modules that provide a range of customisation options. The product is also interoperable with a local customer's specific hardware cryptographic module.

Product Components

The **IP-Granite** product portfolio consists of:

- **IP-Granite** Center – Online central manager
- **IP-Granite** Edge – Site-to-Site VPN and road warrior access server (VPN Gateway)
- **IP-Granite** Nomad – Site-to-site VPN
- **IP-Granite** Buddy (for Windows, Android, Apple and Linux) – VPN Client
- **IP-Granite** DS10 – Custom cryptographic algorithm generator and analyser

IP-Granite Center and **IP-Granite** Edges can also be fitted with a hardware cryptographic module, the QCM-G.

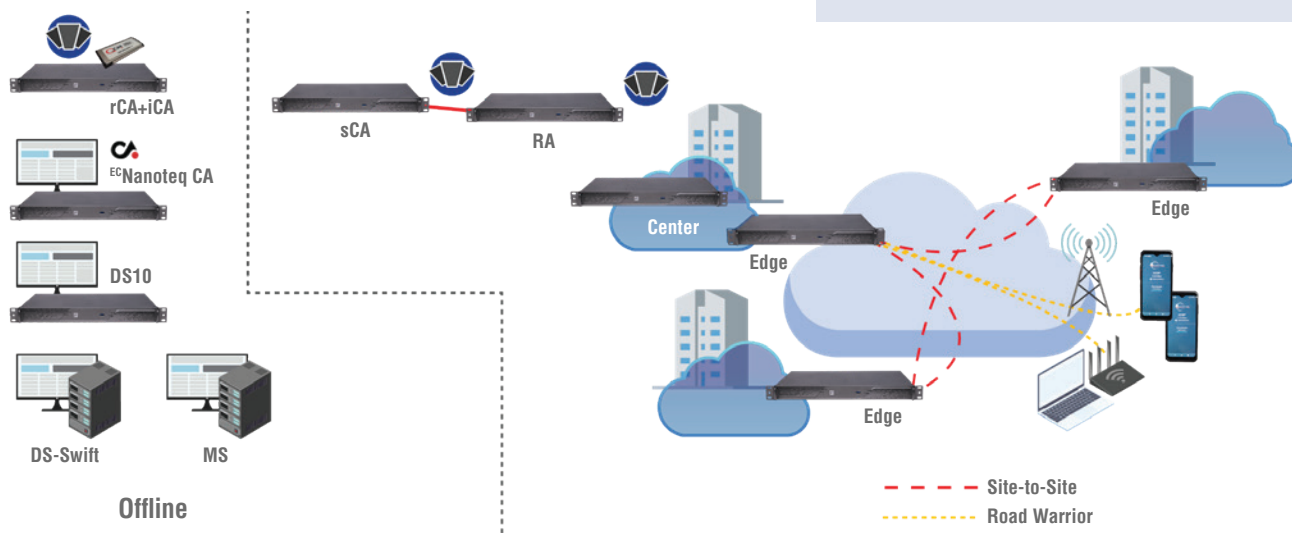
Features

System Management

- Central Management
- Graphical User Interface: **IP-Granite** Center
- Text-based User Interface: **IP-Granite** Edge
- Role-Based Management:
 - User Administrator
 - System Administrator(s)
 - Device Administrator(s)
 - Auditor
 - Privileged User
- Central management of user accounts (2FA, reset, enable/disable, retire)
- Backup and Restore
- Restore to factory settings, zeroise
- Scheduling of configuration updates (**IP-Granite** Edge and Buddy)
- Scheduling of software upgrades (**IP-Granite** Edge and Buddy)
- Status reports
- System reports
- Road Warrior statistics
- Time Synchronization (NTP)
- Local and remote logging
- System monitoring (SNMP v3), different SNMP user accounts
- Health monitoring

VPN Technology

- Site-to-Site VPN: IKEv2, IPsec-based
- Road Warrior: TLS 1.3
- Authentication: X.509v3 Certificate



IP-Granite

Layer-3 Virtual Private network

INTRODUCTION

IP-Granite Center

IP-Granite Center is the central management console. It has a rich graphical user interface that provides capabilities to backup/restore a system, manage users, update configuration remotely as well as system-wide reporting.

All server and cryptographic module configuration and updates are supported over the air via a secure tunnel (IPsec).

The **IP-Granite Center** is a fully installable system, running on the **EC Nanoteq** hardened operating system, nanOS.

The complete VPN configuration for the system is kept on **IP-Granite Center** which allow for rapid replacement of faulty equipment.

IP-Granite Edge

The **IP-Granite Edge** functions as VPN endpoints in a IPsec Site-to-Site VPN. The **IP-Granite Edge** supports software or a dedicated hardware cryptographic module for its IPsec cryptographic operations. The **IP-Granite Edge** also supports a Road Warrior VPN (TLS 1.3), acting as the VPN Gateway to a corporate network. Each gateway enforces policy-based encryption, role-based administration, SNMPv3 monitoring, remote logging and integrated stateful firewall protection.

The **IP-Granite Edge** is fully centrally manageable through the **IP-Granite Center**. The rich text-based user interface allows for initial enrolment, typical support functionality and display of valuable information to administrators.

IP-Granite Nomad

The **IP-Granite Nomad** functions as VPN endpoints in a IPsec Site-to-Site VPN. Each gateway enforces policy-based encryption, role-based administration, SNMPv3 monitoring, remote logging and integrated stateful firewall protection.

The **IP-Granite Nomad** is fully centrally manageable through the **IP-Granite Center**. The rich text-based user interface allows for initial enrolment, typical support functionality and display of valuable information to administrators.

IP-Granite Buddy

Secure access for off-site or roaming personnel is provided through **IP-Granite Buddy**, available for Windows, Android, iOS, macOS and Linux (on request). The client authenticates exclusively via X.509 digital certificates, ensuring cryptographically enforced identity and policy control with the option to authenticate to the server (username and password).

Features include central management (via the **IP-Granite Center**), gateway hunting, dynamic or fixed IP assignment, DNS integration per pool, and configurable inactivity and re-key intervals. All communication uses TLS 1.3 with AES-GCM or AES-CCM (256 bit) encryption and SHA-256/384/512 integrity verification.

IP-Granite DS10

IP-Granite DS10 serves as the cryptographic customisation environment, enabling the generation and verification of custom AES S-Box algorithms. It includes linear and differential cryptanalysis of the generated S-Boxes, multi-user role control, health status reporting, and audit trail generation.

The **IP-Granite DS10** allows for algorithm verification (live capture of encrypted traffic).

Features

Network Topology

- Router-Gateway
- Transparent Firewall (Bridge)
- FailOver clustering

Network, Firewall Technology

- Stateful packet filter firewall
- Static Routing
- Dynamic Routing: OSPF, RIPv2
- VLAN
- IP Masquerading
- Multicast Routing: PIMv2, SSM
- DHCP server
- DHCP client

Site-to-Site VPN

- VPN gateway identified and authenticated based on digital certificate or QCM-G identifier
- Route-based VPN
- Only industry accepted best practice built-in algorithms
- Support for a roaming site
- Support for custom algorithms
- Support for hardware cryptographic module
- Algorithm negotiation

Road Warrior VPN

- Road Warrior user identified and authenticated based on digital certificate
- Additional Authentication to VPN Gateway (username/password)
- Road Warrior user gets assigned to one or more profiles
- Support for multiple Road Warrior IP Pools per gateway
- Fixed and/or dynamic IPs assignment to Road Warrior Clients
- Support for Custom Algorithms
- Algorithm negotiation
- Gateway hunting (dual redundancy)
- Client software:
 - Windows
 - Android
 - iOS (iPhone and iPad)
 - Linux

Custom Algorithm Development

- General:
 - Graphical User Interface
 - S-box generation (AES)
 - Site-to-Site Algorithm
 - Road Warrior algorithm
 - Full logs for auditability
- Custom algorithms applicable to:
 - nanOS (**IP-Granite Center** and **IP-Granite Edge**)
 - **IP-Granite Buddy** (Windows, Android, Apple)
- Custom algorithm qualification

IP-Granite

Layer-3 Virtual Private network

SYSTEM COMPONENTS

External to **IP-Granite** are several supplementary products:

- QCM Management Station (QCM MS) – A comprehensive environment for management of hardware cryptographic modules. In the case of **IP-Granite**, the applicable module is the QCM-G
- QCM Development Station (QCM DS-Swift) – A unique environment dedicated to the customisation of the QCM-G cryptographic modules, used within **IP-Granite**

Remote management of devices is performed by **IP-Granite** Center. The communication between **IP-Granite** Center and the **IP-Granite** Edge devices, is secured through IPsec and requires either a hardware cryptographic module (QCM-G), or X.509 digital certificates. **IP-Granite** seamlessly integrate with:

- KeyStone – An Enterprise Public Key Infrastructure (PKI), developed by **ECNanoteq**
- **ECNanoteq** CA – A single, scaled down Certificate Authority, also developed by **ECNanoteq**

Site-to-Site VPN	
Key exchange	IKEv2 only
IKEv2 encryption	Configurable: - Built-in - Custom - Hardware cryptographic module
	Built-in: - AES CBC (128, 256) - Camellia CBC (128, 256) - AES GCM (128, 256)
IKEv2 Hashing algorithms	Configurable: - Built-in - Hardware cryptographic module
	Built-in: SHA 256, SHA 384, SHA 512
IKEv2 Diffie-Hellman groups	Configurable: - Built-in - Hardware cryptographic module
	Built-in (RSA): DH Group 5/14/16 (MODP-2048/MODP-3072/MODP-4096)
	Built-in (ECC): - NIST (ECP256/384/521) - Brainpool (256BP/384BP/512BP) - Curve25519/Curve448
Authentication	Digital Certificates (X.509)
	Hardware cryptographic module
Auto re-keying	Configurable, IKE SA: 1h-24h
	Configurable, IPsec SA: 10min-8h

IPsec modes	Tunnel mode only
	Enforce ESP with authentication
Differential Service Code Point (DSCP)	Preserve DSCP flags
ESP encryption	Configurable: - Built-in - Custom - Hardware cryptographic module
	Built-in: - AES CBC (128, 256) - Camellia CBC (128, 256) - AES GCM (128, 256)
ESP hashing algorithms	Configurable: - Built-in - Hardware cryptographic module
	Built-in: SHA 256, SHA 384, SHA 512
Differential Service Code Point (DSCP)	Configurable: off, on (10s-10min)
Inactivity period	Configurable: 1min-20min
VPN policies	Route-based VPN only: - Meshed topology - Hub-and-spoke topology (where spokes may be roaming devices) - Individual policies
	Ports:
	• Configurable

IP-Granite

Layer-3 Virtual Private network

SPECIFICATIONS

Road Warrior	
Key exchange	TLS 1.2 and TLS 1.3 - Configurable
Diffie-Hellman groups	Configurable
	Built-in (RSA):
	• DH Group 5/14/16 (MODP-2048/MODP-3072/MODP-4096)
Authentication	Built-in (ECC):
	• secp521r1, secp384r1, secp256r1
	Digital Certificates (X.509) only
Encryption (Control and Data)	Optional to also required Username/password
	Configurable:
	• Built-in
Hashing algorithms (Control and Data)	• Custom
	Built-in:
	• AES CBC (128, 256)
Dead-Peer-Detection (DPD)	• Camellia CBC (128, 256)
	• AES GCM (128, 256)
Polling Delay - Configurable: off, on (10s-10min)	Configurable:
	• SHA 256, SHA 384, SHA 512
	Inactivity Period - Configurable: 1min-20min
Multiple Road Warrior gateways (access points)	Gateway hunting
	Multiple IP pools per gateway
	IP allocation: Configurable:
Fixed only	• Fixed only
	• Dynamic only
	• Fixed and dynamic
DNS configurable per IP Pool	Windows ^[1]
	Android ^[1]
	Apple ^[1]
Road Warrior operating system (IP-Granite Buddy)	Configurable
Protocol/Port	Configurable

PKI and Certificate Support	
Certificate support	X.509 v3 only
	PEM - Decentralised
	PKCS#12 = Centralised
Key generation (Decentralised)	CSR Template
	CSR (PKCS#10)
	RSA
Public/private key pairs	ECC
	Yes, 1-3 levels (root, intermediate, sub-ordinate)
Multiple PKI chains	Yes
	Yes, configurable per service/policy
	KeyStone Enterprise PKI
Interoperable PKI	EC Nanoteq CA

Firewall/Network	
Stateful packet filter firewall	Yes
Per rule logging	Configurable per rule, default is stateful
QoS	Configurable per rule
Network node type	Class based queuing - Hierarchical Fair Service Curve (HFSC)
	Gateway Router
	Bridge (transparent firewall)
Routing	FailOver Cluster
	Configurable:
	• Static routing
Multicast Routing:	• Dynamic routing - OSPF
	• Per interface (private side only): Enabled, Passive or Disabled
	• Authentication (configurable)
Network interface	• Multiple OSPF areas
	• Dynamic routing - RIPv2
	• Per interface (private side only): Enabled, Passive or Disabled
DHCP server (private side only)	• Authentication (configurable)
	• Metric Adjustment (configurable)
	IP Assignment
Static IP	• Static IP
	• Dynamic IP (public side only)
	DHCP server (private side only)

Crypto Support	
Custom software crypto algorithms	Site-to-Site: IKEv2 and ESP
	Road Warrior: TLS (control) and data channel
	Hybrid Site-to-Site VPN policies
Policies configurable to be either built-in algorithms, custom software algorithms, or hardware cryptographic module	Yes, QCM-G
	Updating of:
	• Custom algorithms
Hardware Crypto Module support	• Application firmware
	• User Certificate
	• Policies
Retrieval of Audit Trails	• Blacklists
	Present status information that includes:
	• Temperature out of band
User certificate expiry warning	• Tamper event
	User certificate expiry warning

IP-Granite

Layer-3 Virtual Private network

SPECIFICATIONS

Supportive Services	
Network Monitoring	SNMP v3 (Authentication and Encryption)
	Multiple SNMP users
	Configurable MIB views per user
	Custom MIBs for monitoring IPsec, Road Warrior connections, hardware cryptographic modules
Remote logging	TLS 1.2
	Server authentication
	X.509 certificates (RSA)
Time synchronisation	Network Management Protocol (NTP) supported
Health monitoring	Yes, collects and stores performance data

^[1] Verify with **EC Nanoteq** about the latest version and specification of the latest supported devices

^[2] Verify with **EC Nanoteq** about the traffic profile

Hardware Support and Security	
Supported server models	T-300S, Comply to FIPS 140-2 Level 3
	T-200R, Comply to FIPS 140-2 Level 3
	L-300S, Comply to FIPS 140-2 Level 2
	T-100M, Comply to FIPS 140-2 Level 2
HDD security	Encrypted partitions
	Support for “Zeroise”

System Scaling	
Number of devices	No restriction
Interfaces	Restricted by hardware only
VPN policies (system)	No restriction
Established site-to-site SAs per device	Software cryptography: 512
	Hardware cryptographic module: 512
Local private networks	No restriction
Site-to-Site throughput (IPsec)	T-300S (1Gbps) • ~ Line rate (hardware cryptography) ^[2] • ~ Line rate (AESNI built-in instruction set) ^[2]
	T-200R (100Mbps) • ~ Line rate (hardware cryptography) ^[2] • ~ Line rate (AESNI built-in instruction set) ^[2]
	L-300S (1Gbps) • ~ Line rate (AESNI built-in instruction set) ^[2]
	T-100M (200Mbps) • ~ Line rate ^[2]
Road Warrior pools per device	Multiple
Number of Road Warrior users per device	Recommended pool size of 256
	Maximum pool size of 1000
Simultaneous Road Warrior connections per device	Recommended maximum of 500 simultaneous connected users per gateway
Road Warrior throughput (TLS)	~ 600 Mbps ^[2]
Firewall rules	No restriction